Counteracting Dynamical Degradation of a Class of Digital Chaotic Systems via Unscented Kalman Filter and Perturbation

Yuling Luo[a], Yunqi Liu[a], Junxiu Liu[a], Shunbin Tang[a], Jim Harkin[b], Yi Cao[c]

[a]*School of Electronic Engineering, Guangxi Normal University, Guilin, China*
[b]*School of Computing, Engineering and Intelligent Systems, Ulster University, Northern Ireland, United Kingdom, BT48 7JL*
[c]*Management Science and Business Economics Group, Business School, University of Edinburgh, Edinburgh, EH8 9JS, UK*

Abstract

Theoretically, any chaotic system or chaotic map has ideal complex dynamics. However, because of the finite precision of simulation software and digital devices during implementation, chaotic systems often undergo dynamical degradation, which hinders the further application of digital chaotic systems in many fields. Therefore in this paper, the method based on the perturbation and Unscented Kalman Filter (UKF) theory is designed to counteract the dynamical degradation of digital chaotic systems. Specifically, the UKF algorithm is employed to reinstate the original dynamic performance of the chaotic system, and then perturbation feedback technology is used to cause the chaotic system to obtain strong dynamic performance to resist attacks. The experimental and simulation results demonstrate that this method has good effect on improving the dynamic degradation of digital chaotic map. In addition, the corresponding pseudorandom number generator (PRNG) is constructed via this method, and its randomness is evaluated using the National Institute of Standards and Technology (NIST) SP800-22 and TestU01 test suites. By comparing with other schemes, it can be seen that this PRNG has better performance which illustrates the proposed scheme can be applied in the chaos-based cryptography and

*Corresponding author: Junxiu Liu (j.liu@ieee.org)

utilized in other potential applications.

Keywords: Digital chaotic systems, dynamical degradation, Unscented Kalman Filter, pseudorandom number generator, cryptography

1. Introduction

As a common natural phenomenon, chaos has been applied in a variety of fields, especially for cryptography, image encryption and secure communication, because of the inherent random-like behaviour and other rich properties [1, 2, 3, 4, 5, 6]. Specifically, many chaos-based cryptographic algorithms have been proposed, and the digital implementation of real chaotic systems occupies a pivotal position for the high security of these cryptosystems. In other words, the generation of pseudorandom binary sequences based on chaos is important, and it has been widely utilized in the fields of spread-spectrum communications, error control coding, stochastic computation, data security and so on. Chaotic system is a deterministic system, and it has a kind of random-like movement which can be expressed as the extremely sensitivity to initial conditions and parameters, and the long unpredictable behaviour. Therefore, it can be suitable to design pseudo-random number generators (PRNGs). Then large numbers of pseudo-random number generators derived from chaotic systems have emerged [7, 8, 9, 10, 11, 12]. When an ideal chaotic system is realized via a computer or digital device, it will be discretized, which could result in dynamical degradation of the original system because of the finite precision of these devices, causing the system to develop short-cycle lengths, non-traversal, a low linear complexity and strong correlations [13, 14]. If these drawbacks are ignored, then serious security problems will occur for digital chaos-based applications. Several chaos-based encryption schemes have been compromised and proven to be insecure [15, 16, 17, 18, 19, 20, 21]; for example, the proposed image encryption method in [21] can be broken by a differential chosen-plaintext analysis only through three chosen plain images. Therefore, research on the degradation problem of digital chaotic systems has attracted the attention of scholars.

In general, five methods are widely employed to counteract the dynamical degradation of digital chaos. (a) Methods with higher finite precision [22], which can prevent the dynamical degradation to a certain extent by slowing down the degradation process; however, degradation still occurs. In addition, this method may significantly increase the computational cost, which will limit the practical application of the digital chaotic systems. (b) Cascading multiple chaotic systems [23, 24], which can effectively extend the orbital cycles. However, this method would cause a poor statistical distribution. (c) Switching multiple chaotic systems [25, 26], which aims to expand the time before entering a short cycle by using a superposition of multiple chaotic systems to minimize the degradation. One challenge is the difficulty of designing an approximate and optimal switching rule for multiple chaotic systems. In addition, for each chaotic system used in this switching method, its own degradation is not solved; therefore, the degradation phenomenon is still observed. (d) Error compensation technology [27], which is a good means to ameliorate the performance of the digital chaotic system, although it also exists some limitations. For example, this method is difficult to apply for high-dimensional systems because of the computational complexity. (e) The perturbation method (e.g. in the approaches of [28, 29, 30, 31, 32, 33]), which is a common method and is easy to implement on a digital platform. The perturbed objects include inputs, outputs, and parameters of the chaotic systems, and when the feedback-control algorithm is well designed, the perturbation method can effectively ameliorate the dynamical degradation of the digital chaotic systems without large-scale computing and system integration, which makes it universally applicable to chaos-based cryptosystems and communication [28].

Theoretically, if the discretization and digital implementation of one chaotic system is accomplished under ideal conditions, i.e., without the finite precision problem of the digital platform, then the generated digital sequence must exhibit the basic characteristics of the original system, e.g., good randomness and ergodicity. Otherwise, only if the error of degradation of each state of the digital chaotic system can be appropriately estimated and compensated, the dynam-

ical behaviour of original chaotic system can be recovered to a great extent. In such a case, the generated digital sequence will have good chaotic features, and it is then suitable for the chaos-based cryptosystems and for ensuring a system's security and robustness. As is well known, the Kalman Filter (KF) is an optimal estimation algorithm that optimally estimates the internal state of a dynamical system through the state equation and the observation equation; therefore, it is widely applied in all kinds of fields, such as communication, guidance and navigation. Hypothetically, the degradation of digital chaotic systems may be caused by external noise; as a result, the KF concept can be utilized to resolve the problem of the degradation of digital chaotic systems, and the basic KF algorithm is proposed only for linear systems, however, chaotic systems are nonlinear systems. Of the developed KFs, the Extended Kalman Filter (EKF) and Unscented Kalman Filter (UKF) are adopted for nonlinear systems, where the UKF takes advantage of the unscented transformation (UT) to calculate the statistics of the random variable. The EKF and UKF realize the nonlinear transformation and yield identical performances similar to the basic KF, although the EKF is based on the propagation of linearized dynamics, but this will introduce a significant estimation error and cause high computational complexity and time consumption as the order of the system increases [34]. Therefore, the UKF is widely applied in a variety of nonlinear systems [35, 36, 37].

In our previous work [38], a perturbation method is designed to solve the dynamical degradation of digital Chebyshev chaotic system, but it is only effective for a particular chaotic system (i.e., Chebyshev map). In order to design a universal method and also overcome some drawbacks in the aforementioned approaches, the dynamical degradation of digital chaos systems is analysed and described in this paper, with the error of degradation initially assumed to be the interference result of white noise. The UKF algorithm is used to predict and estimate the approximate ideal digital chaotic sequence (AIDCS). Then, the AIDCS is employed to perturb the actual sequence generated from the chaotic system with an effective precision effect through the feedback-control mechanism. Two examples are experimentally studied and illustrated with the above

method, and the simulation analysis and experimental results demonstrate that there exist an effectiveness, superiority and robustness for this method. Finally, the corresponding PRNG based on the previous example is constructed, and the randomness and security are tested through NIST and TestU01. The results show that the designed PRNG is superior and applicable for chaos-based cryptography and the other potential applications. The contributions of this paper include (a). The approximately ideal digital chaotic sequence can be predicted and estimated by using UKF algorithm. (b). The chaotic attractor structure of original chaotic system is destroyed by using the perturbation method, of which there will be difficultly to reconstruct the phase space property of the system. (c). The improved algorithm has better performance under low precision, which is suitable for the application in the digital devices with finite precision.

The remainder of this paper is organized as follows. Section 2 briefly discusses the degradation theory of digital chaotic systems. Section 3 describes the proposed UKF-based perturbation method in detail. Section 4 presents two examples to check the performance of this method, and Section 5 constructs the corresponding PRNG and analyses the statistical properties. Finally, Section 6 gives the conclusions of this paper.

2. Preliminaries

2.1. Dynamical Degradation of Digital Chaotic Systems

Theoretically, chaotic systems are aperiodic, and the digital chaos systems are normally implemented by using the computers or digital circuit systems in various application fields. However, the computing precisions of the computer or digital circuit are finite, and this leads to short period lengths of digital chaotic systems. This short period phenomenon due to the limited computing precisions are known as the finite precision effect. One example is used in this section to visually show this short-period phenomenon.

Consider that the generic expression of any discrete map of chaos system is

$$X(i+1) = C(X(i)). \tag{1}$$

In the situation of an ideal state, the behaviour of any chaotic system should be sensitive to the initial states, i.e., ergodic, aperiodic, etc. However, if a chaotic system such as that described in Eq. (1) is realized on a digital platform or device (e.g., computer) with finite P-bit precision, the digital output will be limited to a collection that containing 2^P elements, which can be described by

$$\Omega_P = \left\{ (x_i) = k \times 2^{-P} | k = 0, 1, \ldots, 2^P - 1 \right\}, \tag{2}$$

where x_i denotes the output values of the original chaotic system and (x_i) is the decimal part of x_i. Then, the original chaotic system will degrade into

$$X(i+1) = B_P(C(X(i))), \tag{3}$$

where $X(i) \in \Omega_P$, $B_P : \Omega \to \Omega_P$ is a quantization function, which generally has three forms [39]: $floor_P(x) = \lfloor x \cdot 2^P \rfloor / 2^P$, $ceil_P(x) = \lfloor x \cdot 2^P \rfloor / 2^P$, and $round_P(x) = round(x \cdot 2^P)/2^P$. Generally, three situations can lead to the dynamical degradation of digital chaos [40] as follows: first of all, it is the discreteness because the Lebesgue measure of any subset will tend to zero in discrete phase space Ω_P, and then most of the dynamical properties will exist in continuous phase space will become weak and insignificant. Second, the orbit of the generated digital sequence will fall into a periodic orbit because there are only a finite number of isolated elements in the discrete phase space Ω_P. Third, quantization errors occur, and these errors cause the orbit of the generated digital system to deviate far from the original chaotic orbit because of the sensitivity to the initial state values of the chaotic system.

2.2. Remedies and enhancements for dynamical degradation of digital chaotic systems

Chaos systems have an ideal pseudo-random characteristic in theoretical analysis, but the digital performance will be degenerated to some extent when it is implemented on devices with digital platform, i.e., there will be a short period length for the state space, low linear complexity, degraded distribution and strong correlation etc. In order to improve this problem to broaden the

application of the digital chaos, five methods have been recently proposed to address the challenge for the dynamical degradation of digital chaotic systems, that is, using high finite precision chaotic systems, cascading multiple chaotic systems, switching multiple chaotic systems, using error compensation technology and using perturbation method. For instance, the cycling problem of the pseudo-random number can be combatted to any desired degree by using chaos theory [22], and it can be of cryptographic interest as well. In the work of [24], a cascade chaotic system (CCS) is introduced to generate a large number of new chaotic maps, in which two one-dimensional chaotic maps are used to be the seed maps. Although the orbital cycle of the new chaotic system by using CCS is extended, the structure of CCS is still complex compared with the original one-dimensional seed map and so it may be hard to control the dynamical complexity of CCS and some other properties may be ignored to some extent. Besides, a chaotic map based on topological conjugacy is proposed in [26],which aims to expand the time before entering a short cycle by using a superposition of multiple chaotic systems to minimize the degradation. However, the switching rule for the multiple chaotic systems and the degradation of each chaotic system are not solved. In the approach of [27], the performance of digital chaotic systems under the finite computing precision can be improved by using error compensation technology, but the high dimension systems are difficult employed by this method. In addition, perturbing the chaotic systems can also prevent the dynamics degradation of digital chaotic systems, in which the system variables, parameters or both of them can be as the perturbation source. Therefore, the properties of the digital chaotic system are usually depended on the perturbation source. In [30], a variable function is used to replace the input variable of the chaotic system to improve the dynamical degradation of the original digital chaotic system. In the work of [41], a double perturbation method is proposed for reducing the dynamical degradation of the digital Baker map, in which the both state variables and system parameters are perturbed by the digital logistic map.

3. Algorithm Description

Based on the above discussion, to obtain good properties for a digital chaotic system and enhance the security application, a novel method which is based on perturbation feedback technology and UKF theory is designed to counteract the dynamical degradation of digital chaotic systems. Specifically, the UKF algorithm is used to compensate for the quantization error resulting from the finite computing precision, and the perturbation technology is used to adjust and control the dynamic performance to make the chaotic system more resistant to attacks such as phase space reconstruction technology. The corresponding block diagram is shown in Fig.1, which mainly contains two parts: the UKF and perturbation. The UKF includes two major steps: initialization and state estimation, where the initial value and parameters are formed through the initialization stage, and then the new state estimating value $\hat{x}_k$ is obtained through the three steps of calculating sigma points, time update, and measurement update. Then the perturbation method is used to aid generating more random final chaotic system output value z_{k+1}. The main notations in this paper are listed in Table 1.

3.1. UKF Algorithm

The UKF is a good recursive algorithm for estimating internal state of the nonlinear dynamical system through noisy measurements. Specifically, if the dynamical degradation of a digital chaotic system is considered to be caused by noise, which indicates that the finite precision effect can be regarded as noise, then the UKF can be used to evaluate the quantization error resulting from finite computing precision.

A nonlinear discrete system with the state equation and observation equation can be expressed by

$$x_k = f\left(x_{k-1}\right) + w_k, \tag{4}$$

and

$$y_k = h\left(x_k\right) + v_k, \tag{5}$$

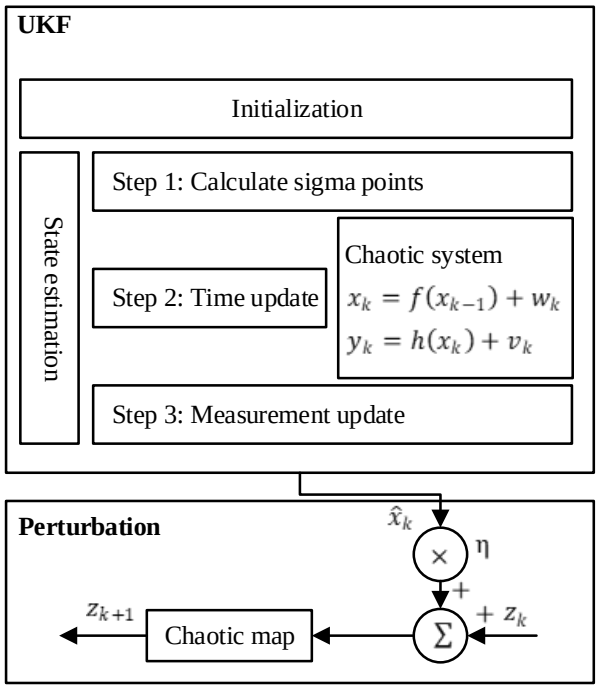

Figure 1: The diagram of the proposed scheme, where x is the unknown state-vector, y is the known observation-vector, and w and v are the assumed independent variables, and $\hat{x}_k$ denotes the corrected state estimate, z_k is the output of the improved system, and η is the controlling parameter.

where k is time step, x is the unknown state-vector, y is the known observation-vector, and w and v are the assumed independent variables, i.e., zero-mean white Gaussian and observation noise vectors, and the corresponding covariances are denoted by Q_k and R_k, respectively.

In (4) and (5), the nonlinear functions $f(\cdot)$ and $h(\cdot)$ capture the state-space and the measurement types, respectively, and in this paper, the function f is set as a digital chaotic system generated under finite P-bit precision and the h function is set as the same digital chaotic system generated under finite P'-bit precision ($P' > P$).

Table 1: The main notations description of this paper.

Notation	Description
χ_{k-1}^{i}	Sigma points
$\chi_{k\|k-1}^{i}$	Propagated state sigma points
$\gamma_{k\|k-1}^{i}$	Propagated output sigma points
$\hat{x}_{\bar{k}}$	Predicted state estimate
$\hat{y}_{\bar{k}}$	Predicted output
$P_{x,k}^{-}$	Predicted covariance
$P_{y,k}$	Output covariance
$P_{xy,k}$	Cross covariance
$\hat{x}_k$	Corrected state estimate
$P_{x,k}$	Corrected covariance
K	Kalman gain

3.1.1. Initialization

First, the initial conditions (e.g., state estimate value $\hat{x}_0$ and covariance P_0) of the filter can be calculated by

$$\hat{x}_0 = E\left[x_0\right], \tag{6}$$

and

$$P_0 = E\left[\left(x_0 - \hat{x}_0\right)\left(x_0 - \hat{x}_0\right)^T\right]. \tag{7}$$

These initial conditions of $\hat{x}_0$ and P_0 are used as the inputs of the filter.

3.1.2. State estimation

The UKF is a UT-based nonlinear KF algorithm, for which the Jacobi matrix does not need to be calculated; therefore, this method can resolve nonlinear functions.

Step 1: Calculate the sigma points. Based on the UT theory, the sigma

points χ^i_{k-1} is defined by

$$\chi^i_{k-1} = \begin{cases} \hat{x}_{k-1}, \;\; i = 0 \\ \hat{x}_{k-1} + \left(\sqrt{(n+\sigma)\, P_{x,k-1}}\right)_i, \;\; i \in [1, n] \\ \hat{x}_{k-1} - \left(\sqrt{(n+\sigma)\, P_{x,k-1}}\right)_i, \;\; i \in [n+1, 2n] \end{cases} \tag{8}$$

where $\hat{x}_k$ is corrected state estimate, n is the length of the augmented, σ is the scaling factor of UT which is set to be $\sigma = \alpha^2(n+\lambda) - n$, $P_{x,k-1}$ is the covariance of x_{k-1}, $(\sqrt{(n+\sigma)P_{x,k-1}})_i$ denotes the ith column of $\sqrt{(n+\sigma)P_{x,k-1}}$, and α is a positive scaling parameter which could be made as small as possible to minimize the effects of higher order ($1e^{-4} < \alpha \leq 1$), λ is a scaling parameter which is usually set to be 0 or $3-n$. Moreover, the corresponding mean weights $W^{(m)}_i$ and variance weights $W^{(c)}_i$ of the χ^i_{k-1} can be calculated by

$$W^{(m)}_0 = \frac{\sigma}{n+\sigma}, \;\; i = 0, \tag{9}$$

$$W^{(c)}_0 = \frac{\sigma}{n+\sigma} + (1 - \alpha^2 + \beta), \;\; i = 0, \tag{10}$$

and

$$W^{(m)}_i = W^{(c)}_i = \frac{1}{2\,(n+\sigma)}, \;\; i \in [1, 2n]. \tag{11}$$

where β is a parameter which minimizes the effects from high order terms, and in this work β is set to be 2.

Step 2: Time update. The $(2n+1)$ sigma points are propagated through the state-output equations of (1) and (2), which are given by

$$\chi^i_{k|k-1} = f(\chi^i_{k-1}), \tag{12}$$

and

$$\gamma^i_{k|k-1} = h(\chi^i_{k|k-1}). \tag{13}$$

Then, the state-output means are calculated by

$$\hat{x}_{\bar{k}} = \sum_{i=0}^{2n} W^{(m)}_i \chi^i_{k|k-1}, \tag{14}$$

and

$$\hat{y}_{\bar{k}} = \sum_{i=0}^{2n} W_i^{(m)} \gamma_{k|k-1}^i. \tag{15}$$

Moreover, the predicted covariance are calculated by

$$P_{x,k}^- = \sum_{i=0}^{2n} W_i^{(c)} [\chi_{k|k-1}^i - \hat{x}_{\bar{k}}][\chi_{k|k-1}^i - \hat{x}_{\bar{k}}]^T + Q_k. \tag{16}$$

Step 3: Measurement update. The output covariance and cross covariance are calculated by

$$P_{y,k} = \sum_{i=0}^{2n} W_i^{(c)} [\gamma_{k|k-1}^i - \hat{y}_{\bar{k}}][\gamma_{k|k-1}^i - \hat{y}_{\bar{k}}]^T + R_k, \tag{17}$$

and

$$P_{xy,k} = \sum_{i=0}^{2n} W_i^{(c)} [\chi_{k|k-1}^i - \hat{x}_{\bar{k}}][\gamma_{k|k-1}^i - \hat{y}_{\bar{k}}]^T. \tag{18}$$

Thus, the corrected state estimate and the corresponding covariance would be given by

$$\hat{x}_k = \hat{x}_{\bar{k}} + K(y_k - \hat{y}_{\bar{k}}), \tag{19}$$

and

$$P_{x,k} = P_{x,k}^- - K P_{y,k} K^T. \tag{20}$$

where K is the Kalman gain, which is given by

$$K = P_{xy,k} P_{y,k}^{-1}. \tag{21}$$

3.2. Perturbation Algorithm

Because of the above-mentioned advantages of the UKF algorithm in terms of prediction, such as the close approximation between the predicted data and the ideal data in the mathematical sense, almost all the characteristics of the improved system could be similar as that of the original chaotic system. Besides, considering the effect of finite precision and to further enhance the applicability

in cryptography, the predicted chaotic system in the terms of UKF is then feedback and disturbed. The specific implementation is described by

$$z_{k+1} = mod\left(B_{P'}(f\left(z_k + \eta * \hat{x}_k\right)), 1\right), \tag{22}$$

where $mod(A, B)$ returns the modulus after division of A by B, and $B_{P'} : \Omega \to \Omega_{P'}$ is a universal function of a quantization process, which is defined by $B_{P'}(.) : floor_{P'}(.)$, and the output $\hat{x}_k$ of the predicted chaotic system is utilized to disturb the input of the original chaotic system, z_k is the output of the improved system, η is the controlling parameter and $\eta = e^{\lambda}$, and λ is the exponential factor.

4. Scenarios

In this section, experiments are conducted on two examples to confirm the performance of the proposed method. In other words, the proposed method is applied to the 1-D Chebyshev map and the 3-D hyperchaotic Henon map to test its effectiveness.

4.1. Example 1: 1-D Chebyshev Chaotic Map

Consider the Chebyshev map [38], which is given by

$$x_{i+1} = \cos\left(\beta \cdot \arccos x_i\right), \qquad x_i \in [-1, 1], \tag{23}$$

where when the parameter $\beta \geq 2$ it would be chaotic in an ideal situation. Moreover, if the Chebyshev map is realized with P-bit finite precision, the orbit of its state space will be confined to the discrete set of the Eq. (2).

As a result, the original chaotic state would degrade into the digital system of

$$x_{i+1} = B_P\left(\cos\left(\beta \cdot \arccos x_i\right)\right), \tag{24}$$

where $B_P : \Omega \to \Omega_P$ is a universal function of a quantization process, which is defined by $B_P(\cdot) = floor_P(\cdot)$ in this approach.

According to the UKF theory, the specific state equation and observation equation can be calculated by

$$x_k = f(x_{k-1}) = B_P(\cos(\beta \cdot \arccos x_{i-1})), P = 8, \tag{25}$$

and

$$y_k = h\left(x_k\right) = B_{P'}\left(x_k\right),\ P' = 16. \tag{26}$$

Then, the output $\hat{x}_k$ of the predicted system is utilized to disturb the input of the original chaotic system. Therefore, the improved digital system can be given by

$$z_{k+1} = mod(B_{P'}(cos(6 * \arccos(z_k + \eta * \hat{x}_k))), 1) * 2 - 1, P' = 16. \tag{27}$$

4.1.1. Parameter Selection

As discussed above, the dynamical behaviour of the improved digital Chebyshev map mainly depends on the exponential factor λ of the controlling parameter η. Therefore, the impact of exponential factor λ on the dynamics of the Chebyshev map is first discussed in accordance with the approximate entropy to check the degree of complexity of a dynamical system. As we all known, approximate entropy was firstly proposed by Pincus [42] to measure the complexity of time series and the randomness of binary sequence. The greater the approximate entropy, the higher the complexity of the system. The test process of approximate entropy can be described in the following steps.

Step 1. Taken a 1D discrete-time sequence with a length of N as an example, which is defined as $ts(i) = 1, ...N$, then rebuild it into an m-dimensional vector $X_i = ts(i), ts(i+1), \ldots ts(i+m-1)$, where $i = 1, 2, ..., N - m + 1$.

Step 2. The distance between two vectors X_i and $X_j (j = 1, 2, \ldots N - m + 1, j \neq i)$ is computed, and the maximum absolute value of the corresponding elements between any two different vectors can be described by

$$d_{ij} = max|ts(i+j) - ts(j+k)|, k = 0, 1, ..., m-1. \tag{28}$$

Step 3. A threshold value $\gamma_{tv} \in (0.2, 0.3)$ is given, and then the number of $d[X(i), X(j)] < \gamma_{tv}$ is counted and denoted as ∂_n. Moreover, the resulting

number $C_i^m(\gamma_{tv})$ can be written by

$$C_i^m(\gamma_{tv}) = \frac{1}{N-m}\partial_n, k = 0, 1, ..., m-1. \tag{29}$$

Step 4. Transform $C_i^m(\gamma_{tv})$ into logarithmic form and the average value can be obtained by

$$\phi^m(\gamma_{tv}) = \frac{1}{N-m+1}\sum_{i=1}^{N-m+1} lnC_i^m(\gamma_{tv}), k = 0, 1, ..., m-1. \tag{30}$$

Step 5. m is added by one, and repeat the above steps, the corresponding $C_i^m(\gamma_{tv})$ and $\phi^m(\gamma)$ are obtained again.

Step 6. The approximate entropy can be computed by employing $\phi^{m+1}(\gamma_{tv})$ and $\phi^m(\gamma_{tv})$:

$$ApEn = \sum_{N\to\infty}[\phi^m(\gamma_{tv}) - \phi^{m+1}(\gamma_{tv})]. \tag{31}$$

The experimental result is shown in Fig. 2, which describes the approximate entropy trend with different λ values. Fig. 2 shows that the approximate entropy of the improved digital map becomes larger sharply as $\lambda \in (-10, -1)$, and it leads to stable when λ exceeds a critical value ($\lambda = 4$). As mentioned in the approach of [38], the approximate entropy is closely related to the space distribution of system; therefore, it will achieve the maximal value when the distribution of the assumed random sequence is uniform. Based on this theory, we analyse the distribution error by comparing the value of the approximate entropy of the system. As shown in Fig. 2, the distribution error becomes increasingly small with increases in λ, and the system will enter into a relatively stochastic situation as λ exceeds the critical value ($\lambda = 4$).

Based on this analysis of the approximate entropy, the exponential factor λ of the controlling parameter η is selected from the interval [0, 8], and experiments are performed to test the evolution of the controlling system in phase space. The experimental results are shown in Fig. 3, and they indicate that the regular state pattern will be confused and then finally distributed uniformly with an increase of λ. Specifically, when the exponential factor λ is equal to 5, the phase space distribution gradually becomes uniform and resembles random noise, which shows that the system is becoming random.

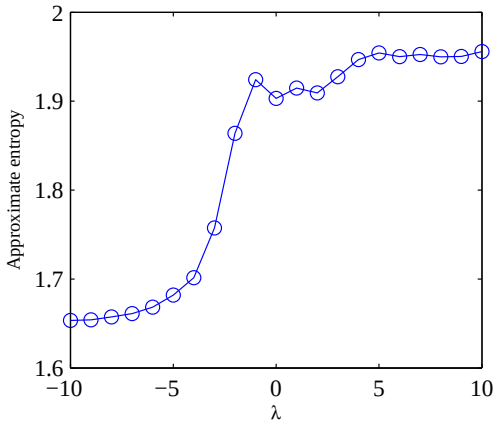

Figure 2: Approximate entropy trend with parameter λ.

Without a loss of generality, the frequency distribution (FD) is further used to test the effect of the range of the exponential factor λ on the system. As shown in Fig. 4, the FD simultaneously changes as λ changes. Specifically, the FD becomes increasingly uniform as λ grows and incline to stabilize when λ exceeds the threshold $\lambda = 5$.

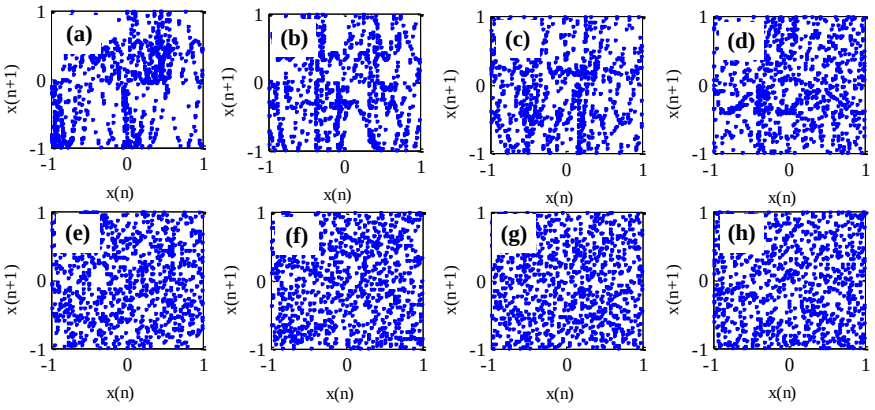

Figure 3: Chaotic attractors of the improved Chebyshev map with different λ values. (a). $\lambda = 1$. (b). $\lambda = 2$. (c). $\lambda = 3$. (d). $\lambda = 4$. (e). $\lambda = 5$. (f). $\lambda = 6$. (g). $\lambda = 7$. (h). $\lambda = 8$.

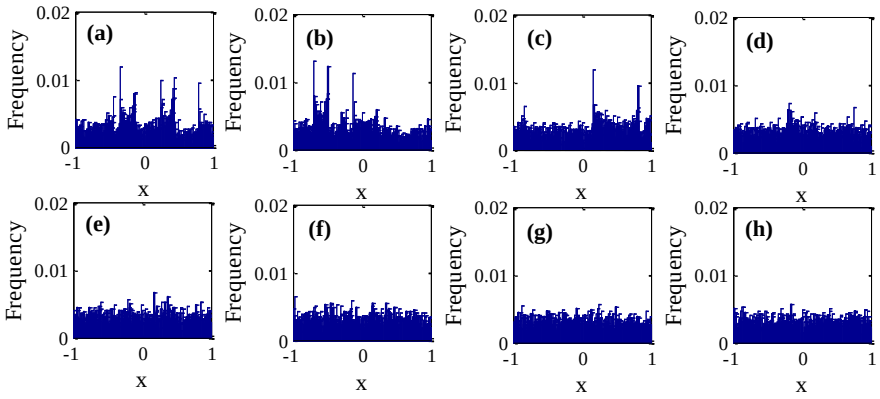

Figure 4: Frequency distributions of the improved Chebyshev map with different λ values. (a). $\lambda = 1$. (b). $\lambda = 2$. (c). $\lambda = 3$. (d). $\lambda = 4$. (e). $\lambda = 5$. (f). $\lambda = 6$. (g). $\lambda = 7$. (h). $\lambda = 8$.

Lyapunov exponent is an important qualitative and quantitative characterization to evaluate the convergence and divergence degree of two adjacent phase space tracks of the dynamical system to some extent.[43, 44]. Generally, when a system has a positive Lyapunov exponent, it demonstrates that two orbits will exponentially increase even if there is small difference for initial values, and it also shows the system is chaotic. In this paper, the largest Lyapunov exponents are calculated by the Wolf method with the change of system parameters λ, and Fig. 5 shows the experimental data. From Fig. 5, it can be seen the improved Chebyshev system is chaotic under the certain parameters.

4.1.2. Dynamical Behaviour

The complexity of a time series can reflect the dynamical behaviour, and it can be verified through approximate entropy which can report the randomness of a binary sequence. Here, it is also used to test the dynamical behaviour of the original Chebyshev and the improved systems. As shown in Fig. 6, the approximate entropy of the improved Chebyshev system is larger than that of the original Chebyshev system, which illustrates that this method can effectively improve the dynamical behaviour of the original system.

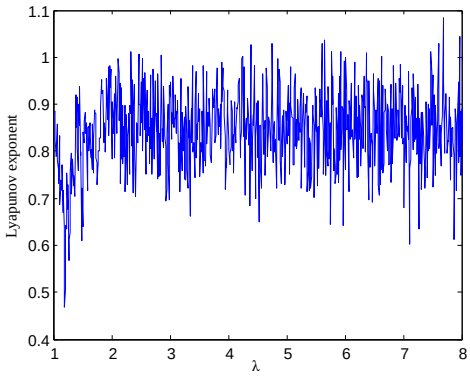

Figure 5: Lyapunov exponents of the improved Chebyshev map with different λ.

Generally, the chaotic attractor has a specific geometric shape for each chaotic system, and the complexity degree can reflect the confusion to some extent. The chaotic attractor of Chebyshev map is likely a trigonometric function, and its state space is in the range of [-1, 1] (see Fig. 7(a)). After the process of prediction and perturbation, the system orbit of the map constantly diffuses and folds and finally becomes irregular and breaks the correlation between two adjacent states (see Fig. 7(b)). This correlation is uniform, which means that it is likely a noise signal. Accordingly, reconstructing the mathematic structure of the original map is impossible.

The auto-correlation function describes the degree of dependence between two state values of any one sequence, and the cross-correlation function describes the degree of dependence between two state values of different sequences. Ideally, the auto correlation function of any random series should be a delta function, and the cross-correlation function should be zero. As shown in Fig. 8, the correlation characteristics of the improved systems are good.

The FD of a state value of any system can reflect the arbitrariness degree. From the Fig. 9(a), it can be seen that the FD function of the original Chebyshev system is relatively uniform but emerge a 'U'-type invariant density function because of the frequency at -1 and 1. However, Fig. 9(b) shows that the dete-

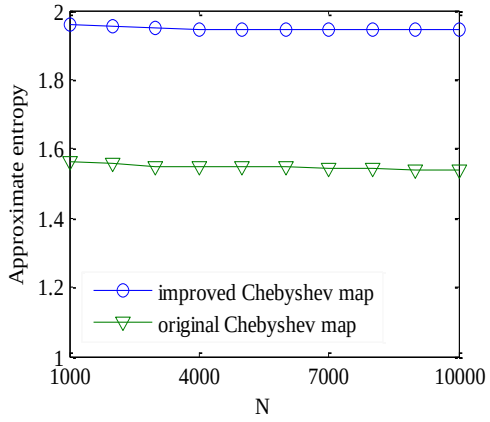

Figure 6: Approximate entropies.

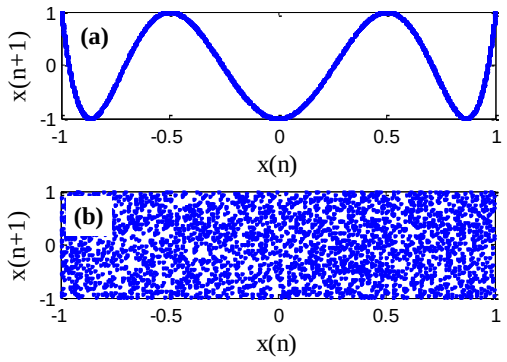

Figure 7: Chaotic attractors of the (a) digital Chebyshev map and (b) improved Chebyshev map.

rioration effect is weakened and the FD function is smoothed and homogenized by using the aforementioned improved method. Therefore, the frequency attack can be effectively overcome by means of this proposed UKF-based perturbation method.

Recurrence plot (RP) analysis is also an important trick to visualize the phase space recursion [45]. As for a time series $\{x_1, x_2, ..., x_n\}$, the reconstructed space vector is $X_i = (x_i, x_{i+\tau}, ..., x_{i+(m-1)\tau})$, then the RP of a trajectory $x_i \epsilon R^d$

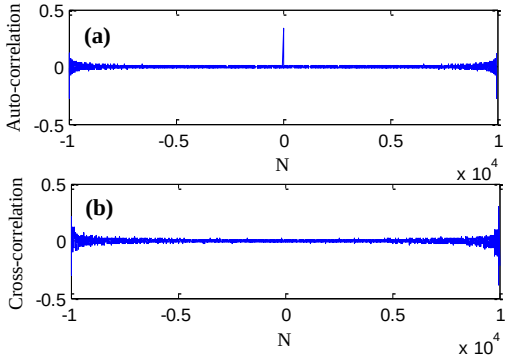

Figure 8: Auto-correlation (a) and cross-correlation (b) of the sequence of a digital improved Chebyshev map.

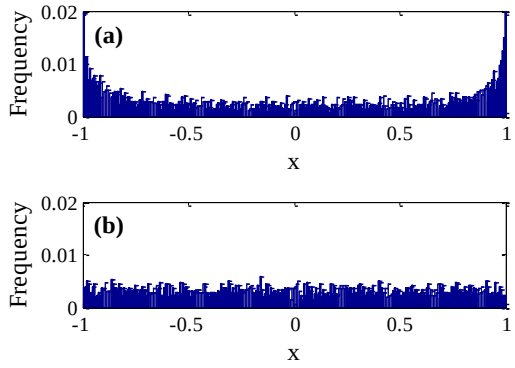

Figure 9: Frequency distributions of the (a) original digital Chebyshev map and (b) improved Chebyshev system.

can be given by the matrix

$$R_{i,j}(\varepsilon) = \theta(\varepsilon - \parallel X_i - X_j \parallel), i, j = 1, ..., N, \tag{32}$$

where N is the number, ε is a threshold distance, $\parallel \cdot \parallel$ is a norm, and $\theta(\cdot)$ is Heaviside function, in that, $\theta(\cdot) = 0$, if $x < 0$, and $\theta(\cdot) = 1$ otherwise. A RP can be obtained by drawing $R_{i,j}(\cdot)$ on a two-dimensional $i-j$ graph, and the specific process is as follows: when the state X_i is close to X_j, i.e. $\parallel X_i - X_j \parallel \leq \varepsilon$, then $R_{i,j}(\cdot) = 1$, and black dots are visualized in RP flat; otherwise, $R_{i,j}(\cdot) = 0$ and

white dots are visualized in RP flat. Therefore, RP can be viewed as a visual inspection of the high-dimensional phase space trajectory, in that, RP could give a hint for the time evolution of a trajectory.

The RP of stationary signal should be evenly distributed, in that, if some straight lines exist to be parallel to the main diagonal line, it means that the signal is not completely stable. For example, white noise is completely stationary, so its coordinates of the time series are full of RP distribution. And the RP distributions of the original Chebyshev system and improved Chebyshev system are shown in Fig. 10(a) and Fig. 10(b). The results show that compared with Fig. 10(a), Fig. 10(b) does not obviously occur short lines to be parallel to the main diagonal. Therefore, the PR result illustrates that the improved Chebyshev system is as random as white noise.

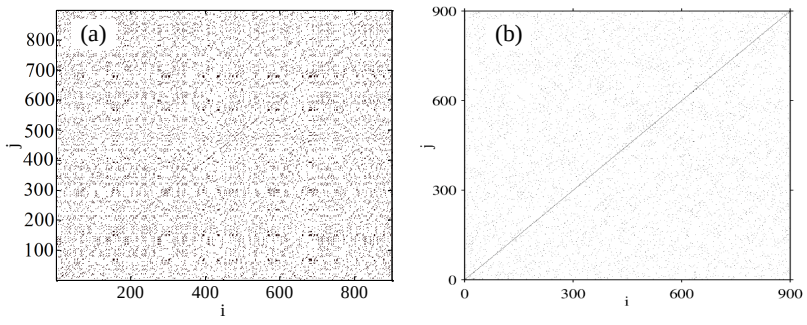

Figure 10: (a)Recurrence plot (RP) of original Chebyshev system.(b)Recurrence plot (RP) of improved Chebyshev system.

4.1.3. Performance Comparison of Different Remedies

To better illustrate the superiority of the proposed method, the simulation results (such as attractor distribution, FD, and approximate entropy) obtained through the proposed method in this paper are compared with those of three other methods, which are used to counteract the dynamical degradation of a digital Chebyshev map. Specifically, the approach in [28] proposed a novel perturbation method that is on the basis of tent and Chebyshev map; the approach

in [30] used the variable function to be the input data of the Chebyshev map, and the original system structure remained unchanged; and the approach in [10] constructed a new multi-delayed Chebyshev map.

As shown in Fig. 11, although the attractor distributions of the four methods are all more complicated than the original parabolic shape, which makes the generated sequences random and hard for an intruder to predict, the attractor distribution of this method is more uniform than those of the other three methods. Therefore, the attractor is likely a noise pattern, which means that the correlation between adjacent states is weak and can obtain better random sequences for direct application in chaos-based digital information security.

The FDs of the four modified digital Chebyshev maps are shown in Fig. 12. To better show the results, the state space of [-1, 1] is divided into 200 equal subintervals. The results illustrate the improved design in this paper has a better improvement effect because the whole FD is almost ergodic and homogeneous. However, the FDs of the other three methods still appear to be 'U'-type invariant density functions, which may be uniform except at the two endpoints, -1 and 1.

Moreover, as shown in Fig. 13, the approximate entropy of the proposed system in this paper is better than those of other three methods. Therefore, compared with the other three methods, this improved method can make the digital chaotic system more complicated to some extent, which is better for the digital application of the Chebyshev map.

4.2. Example 2: Hyperchaotic Henon Map

Consider that the generalized Henon map [39] is

$$\begin{cases} x_{k+1} = a - y_k^2 - b \times z_k \\ y_{k+1} = x_k \\ z_{k+1} = y_k \end{cases} \tag{33}$$

where a and b are the system parameters, and when a=1.76 and b=0.1, the system is a hyperchaotic system. If this hyperchaotic Henon system is realized

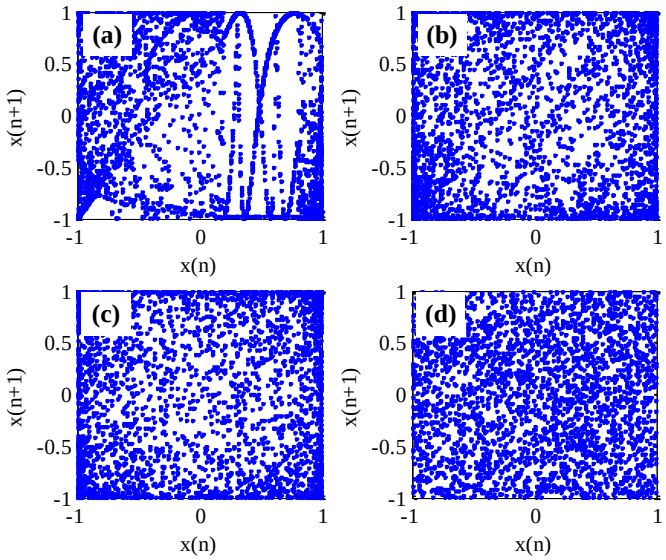

Figure 11: Attractors of different modified digital Chebyshev maps. (a). Ref. [28]. (b). Ref. [30]. (c). Ref. [10]. (d). Improved system.

with a finite precision of P bits, then the state space of system will be degraded into the situation of

$$\begin{cases} x_{k+1} = B_P\left(a - y_k^2 - b \times z_k\right) \\ y_{k+1} = B_P\left(x_k\right) \\ z_{k+1} = B_P(y_k). \end{cases} \tag{34}$$

Similarly, the improved digital system will be given by

$$\begin{cases} x_{k+1} = B_P(a - (4 \cdot \mathrm{mod}(B_P(\bar{y}_k), 1) - 2)^2 \\ \qquad\qquad -b \times (4 \cdot \mathrm{mod}(B_P(\bar{z}_k), 1) - 2)) \\ y_{k+1} = 4 \cdot mod(B_P\left(\bar{x}_k\right), 1) - 2 \\ z_{k+1} = 4 \cdot mod(B_P\left(\bar{y}_k\right), 1) - 2 \end{cases} \tag{35}$$

where $\bar{x} = x_k + \eta \cdot \hat{x}_k$, $\bar{y} = y_k + \eta \cdot \hat{y}_k$ and $\bar{z} = z_k + \eta \cdot \hat{z}_k$ ($\hat{x}_k$, $\hat{y}_k$, and $\hat{z}_k$ are the outputs of the predicted chaotic system), and $B_P : \Omega \to \Omega_P$ is a common quantization function, such as $B_P\left(\cdot\right) = floor_P\left(\cdot\right)$, in this approach.

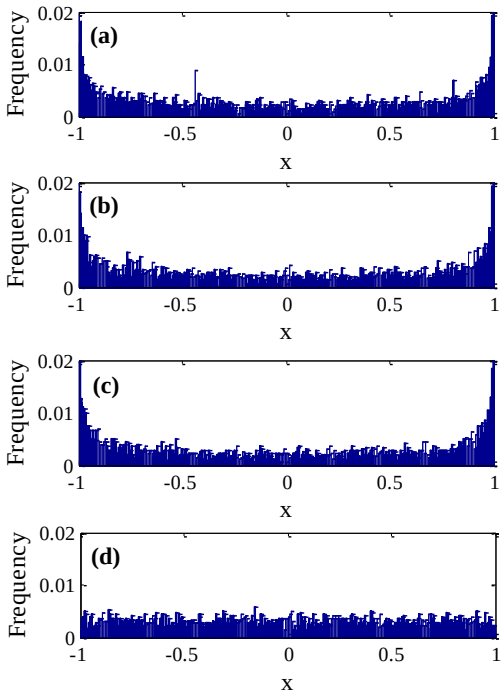

Figure 12: Frequency distributions of different modified digital Chebyshev maps. (a). Ref. [28]. (b). Ref. [30]. (c). Ref. [10]. (d). Improved system.

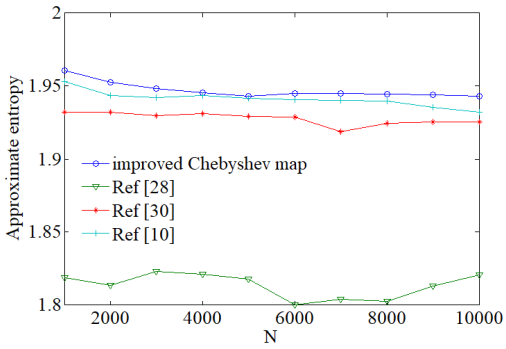

Figure 13: Approximate entropies of different modified digital Chebyshev maps.

The experimental phase diagrams are shown in Fig. 14. Fig. 14(a) shows the original hyperchaotic Henon map and 14(b) displays the chaotic attractor structure of digital hyperchaotic Henon map under the precision of 6. Figure 14(a) and (b) are same as Ref. [39], while Fig. 14(c) is the chaotic attractor structure of chaotic system by using this improved algorithm under the precision of 6, in which the attractor distribution is more complex to be likely a honeycomb. It is indicated that the proposed improved algorithm has more excellent performance than Ref. [39].

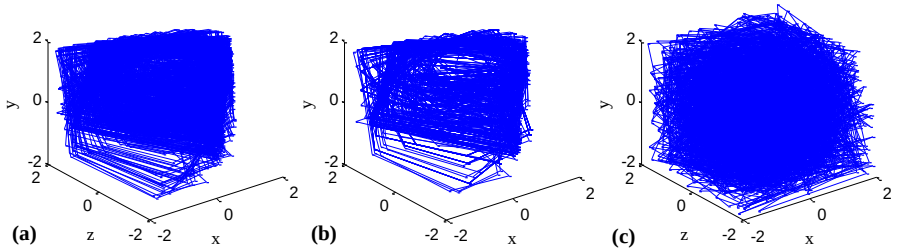

Figure 14: Attractors of three comparative systems with randomly chosen initial values. (a) Hyperchaotic Henon map. (b) Digital generalized hyperchaotic Henon map with computer precision P=6. (c) Improved hyperchaotic Henon map with computer precision P=6.

Moreover, experimental result about the approximate entropy is shown in Fig. 15, which demonstrates the approximate entropy of the improved digital system gradually becomes closer to the value of 2.63 even though under a lower precision, and moreover it is still much larger than that of the original Henon system.

Frequency distributions (FD) of the original Henon map and the improved Henon map under a low precision are shown in Fig. 16(a) and (b). In this test, the interval $[-2, 2]$ of the x-axis is divided into 200 equal sub-intervals. The results show that the FD of the original hyperchaotic Henon map is not uniform, whereas the FD obtained using UKF-based perturbation feedback technology is very uniform.

In addition, the NIST test suite, i.e., it is an industry standard of random test through 15 tests, is used to verify the performance of the designed binary

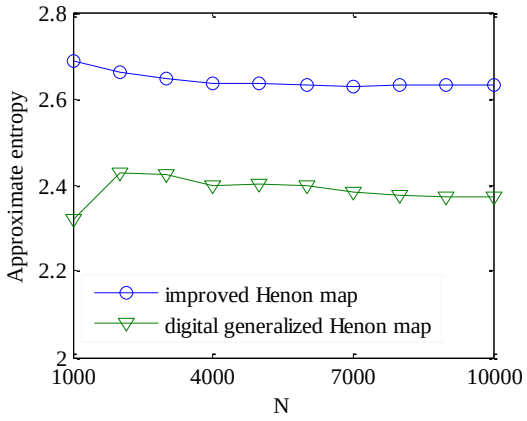

Figure 15: Approximate entropies of the digital generalized Henon map and improved Henon map.

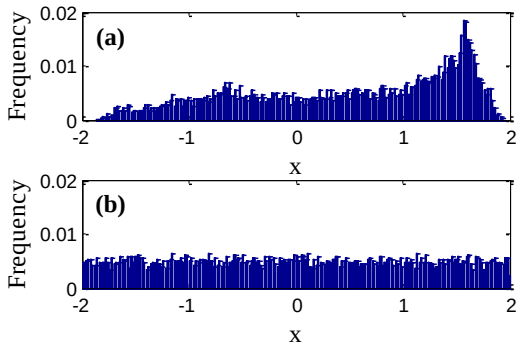

Figure 16: Frequency distributions of the digital generalized: (a) Henon map; (b) Improved Henon map.

sequence. Specifically, these 15 tests focus on evaluating the same sequence with n bits to obtain a p-value. For the specific experiment, the binary sequence is with a length of 10^7 bits. The significance level α is set at 0.01, which is commonly used in the NIST test. The result demonstrates that the binary sequence
385 can pass the statistical test if p-value $\geq \alpha$; otherwise, it fails. Table 2 summarizes the experimental result and it illustrates the binary sequence generated by the improved Henon map can pass all the standard, which means the binary

sequence is randomness to some extent.

5. Pseudo-Random Number Generator (PRNG) and Performance Analysis

5.1. Proposed PRNG

The PRNG is a crucial element of a variety of digital applications, such as cryptology, spread-spectrum communication, computer games, and artificial intelligence. Taking the UKF-based improved digital Chebyshev map as an example, a PRNG is briefly constructed by

$$b\left(z_i\right)=\begin{cases}0, & if \;\; z_i \in (-0.5,\; 0.5) \\ 1, & if \;\; z_i \in [0.5,\; 1) \;\; or \;\; z_i \in (-1,\; -0.5]\end{cases} \tag{36}$$

where $z_i \in [-1, 1]$ is the state value of the improved Chebyshev map in (27).

5.2. Linear Complexity

Linear complexity is another index and it also reflects the complexity of a sequence to a large extent. Ideally, if the length of a binary sequence is n, its expected linear complexity would be $n/2$. The linear complexity of this PRNG in (36) is shown in Fig. 17, which illustrates that the result approximately equal to the straight line of $n/2$. Therefore, the sequence from the proposed PRNG has good linear complexity.

5.3. Statistical Test

The statistical test is another basic criterion with which to measure the performance of a PRNG, and an ideal PRNG should pass all tests in the corresponding standard test suites. As for the proposed PRNG, the NIST SP 800-22 test suit [46] and TestU01 [47] software library are employed to test the statistical performance for the PRNG by using the UKF-based perturbation feedback technology.

First, the SP800-22 testing experiment is performed, and Table 3 summarizes the results. Specifically, there are 10^3 different binary sequences to be generated

Table 2: Uniformity of the p-value under each test in the NIST suite (improved hyperchaotic Henon map)

Statistical tests	p-value	Conclusion
Frequency test	0.574986	pass
Block Frequency test	0.395625	pass
Cusum test mode 1 (forward)	0.798332	pass
Cusum test mode 2 (reverse)	0.629204	pass
Rank test	0.462431	pass
Long runs of ones test	0.379543	pass
Runs test	0.645132	pass
FFT test	0.785632	pass
Non-overlapping Templates test	0.989489	pass
Overlapping Template test	0.682447	pass
Universal test	0.486281	pass
Approximate entropy	0.347256	pass
Random Excursions	0.769701	pass
Random Excursions Variant	0.774092	pass
Linear Complexity (M=500)	0.520404	pass
Serial (m=16)	0.379513	pass

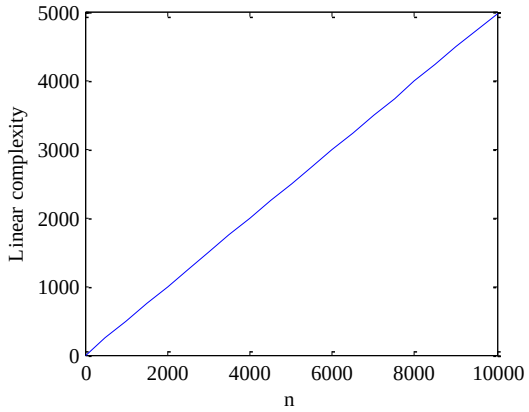

Figure 17: Linear complexity of the generated binary sequence.

through altering initial value of the improved system, where the length of each sequence is supposed to be 10^7 bits. From Table 3, it can be seen that the binary sequence can pass all the standard of test suite, so it has good statistical properties.

Furthermore, TestU01, which offers a collection of utilities to test random number generators, is used to evaluate the PRNG. This test provides several batteries of tests, and each battery consists of multiple tests and focuses on different performance aspects. Here, only the Small-Crush battery and the Crush battery that included in the TestU01 test suite are utilized to examine the randomness and security of this PRNG. Specifically, each sequence is set to a length of 2^{29} bits (4 GB of data) or 2^{35} bits (256 GB of data). Similarly, each statistical test generates a p-value, which is used to judge whether the PRNG passes the test or not, i.e., if it is in the range of [0.001, 0.999], the PRNG can pass the test. Table 4 lists the failure counts of tests in TestU01 for the proposed PRNG and other several schemes, including the Chebyshev map, the schemes in [9], [38], [48], and [49], the scheme of Li et al. [8] and the rand function. From Table 4, it can be seen that our PRNG has a relatively good statistical performance.

Table 3: Uniformity of the p-value under each test in the NIST suite (improved Chebyshev map).

Statistical tests	p-value	Conclusion
Frequency test	0.629806	pass
Block Frequency test	0.803342	pass
Cusum test mode 1 (forward)	0.643918	pass
Cusum test mode 2 (reverse)	0.613746	pass
Rank test	0.681142	pass
Long runs of ones test	0.362045	pass
Runs test	0.341994	pass
FFT test	0.963403	pass
Non-overlapping Templates test	0.990697	pass
Overlapping Template test	0.733140	pass
Universal test	0.078714	pass
Approximate entropy	0.608828	pass
Random Excursions	0.908554	pass
Random Excursions Variant	0.951556	pass
Linear Complexity (M=500)	0.295124	pass
Serial (m=16)	0.124101	pass

Table 4: Statistical test comparison of the proposed PRNG with other PRNGs (failure counts are given).

System	Small-Crush (15)	Crush (144)
Our PRNG	2	23
Chebyshev map	15	139
Scheme in Ref. [38]	2	37
VPCMDP [48]	3	15
Scheme in Ref. [49]	2	12
Scheme in Ref. [9]	3	19
Scheme of Li et al. [8]	15	144
Rand function	7	63

5.4. Information Entropy Analysis

Information entropy [50] reflects the randomness of stochastic data from the perspective of information probability. Suppose the information source to be m; then, its information entropy would be defined by

$$H(m) = \sum_{i=0}^{2^L-1} p(m_i) \log_2 \frac{1}{p(m_i)}, \tag{37}$$

where L is the information length, $p(m)$ represents the probability of some symbol m. Ideally, we can get a maximum information entropy 8 if $L = 8$ for a random sequence.

In terms of (37), each computing results of different sequence generated by the same system only with different initial values are shown in Table 5. The data shows that each entropy is very close to 8, so it indicates that this PRNG is independent of the initial value and the proposed system has strong ability to resist information leakage.

5.5. Key Space and Sensitivity Analysis

For the application of the PRNG in information security, the key space and sensitivity are two significant targets to be sure the system safe. First, the

Table 5: Information entropy results for different initial values.

$m0$	0.38	0.78	-0.59
$H(m)$	7.9813	7.9813	7.9813

parameters β and λ and the initial value x_0 of the system can be determined as keys of this PRNG. Specifically, the parameter β is in the range of $[2, +\infty)$, λ is in the range of $[7, +\infty)$ and the initial value x_0 is in the range of $(-1, 1)$. If the precision is 10^{-15} (precisely 2^{52} for 64-bit double float) [51], then the size of key space would be approximately $2 \times 2^{52} \times 2^{52} \times 2^{52} = 2^{157}$. In general, such a large key space can withstand attacks.

Further, key sensitivity is tested through experiments. For a binary sequence, a change rate of 50% will occur if there is a tiny difference for the parameters or initial value in the ideal situation. In the simulation experiment, the initial value and system parameters are slightly changed with 10^{-15} precision, and the change rate H is calculated between the original binary sequence and the new binary sequence. Specifically, the length of each binary sequence is set to 1000000 bits. The experimental results are summarized in Table 6. The change rate in different situations is approximately 50%, which means the system is extreme sensitive to the initial value x_0 and parameters β and λ.

Table 6: Results of the test for key sensitivity.

Change for keys	H
$x_0 = 0.3891 + 10^{-15}$, $\beta = 6$, $\lambda = 7$	50.55%
$x_0 = 0.3891$, $\beta = 6 + 10^{-15}$, $\lambda = 7$	50.24%
$x_0 = 0.3891$, $\beta = 6$, $\lambda = 7 + 10^{-15}$	49.06%

6. Conclusion

By combining the UKF and a perturbation algorithm, a novel method has been proposed in this work to resolve the dynamical degradation of chaotic system. It can prevent the dynamical degradations of digital chaotic systems. Results show that the proposed method can not only enhance the complexity of nonlinear dynamical behaviours of a digital chaotic system but can also make the improved digital chaotic system possess better ergodicity, better statistical characteristics, and a phase space with no pattern. A high credibility of randomness PRNG has been constructed by using the improved chaotic system and the testing results show the good performance outputs. In addition, the performance comparisons with other synchronization schemes further reveal the superiority of this method. All of these results demonstrate that the proposed method can be used in potential applications such as cryptography due to its cryptographic properties.

Acknowledgements

This research was supported by the National Natural Science Foundation of China under Grants 61801131 and 61661008, the funding of Overseas 100 Talents Program of Guangxi Higher Education, 2018 Guangxi One Thousand Young and Middle-Aged College and University Backbone Teachers Cultivation Program.

References

[1] F. Dachselt, W. Schwarz, Chaos and cryptography, IEEE Transactions on Circuits and Systems I Fundamental Theory and Applications 48 (12) (2002) 1498–1509.

[2] X. Wang, W. Zhang, W. Guo, Secure chaotic system with application to chaotic ciphers, Information Sciences 221 (1) (2013) 555–570.

[3] Y. Luo, M. Du, A self-adapting image encryption algorithm based on spatiotemporal chaos and ergodic matrix, Chinese Physics B 22 (8) (2013) 316–324.

[4] Y. Luo, L. Cao, S. Qiu, H. Lin, J. Harkin, J. Liu, A chaotic map-control-based and the plain image-related cryptosystem, Nonlinear Dynamics (2015) 1–18.

[5] Y. Luo, TangShunbin, F. Jiang, J. Liu, A Double-Image Encryption Scheme Based on Amplitude-Phase Encoding and Discrete Complex Random Transformation, IEEE Access 6 (1) (2018) 77740–77753.

[6] M. Asgari-chenaghlu, M.-a. Balafar, A novel image encryption algorithm based on polynomial combination of chaotic maps and dynamic function generation, Signal Processing 157 (1) (2019) 1–13.

[7] T. Addabbo, M. Alioto, A. Fort, A. Pasini, S. Rocchi, V. Vignoli, A class of maximum-period nonlinear congruential generators derived from the rényi chaotic map, IEEE Transactions on Circuits and Systems I Regular Papers 54 (4) (2007) 816–828.

[8] C. Li, J. Chen, T. Chang, A chaos-based pseudo random number generator using timing-based reseeding method, in: IEEE International Symposium on Circuits and Systems, 2006, pp. 3277–3280.

[9] X. Wang, X. Qin, A new pseudo-random number generator based on cml and chaotic iteration, Nonlinear Dynamics 70 (2) (2012) 1589–1592.

[10] L. Liu, S. Miao, M. Cheng, X. Gao, A pseudorandom bit generator based on new multi-delayed chebyshev map, Information Processing Letters 116 (11) (2016) 674–681.

[11] M. Garcia-bosque, A. Pérez-resa, C. Sánchez-azqueta, C. Aldea, S. Celma, Chaos-Based Bitwise Dynamical Pseudorandom Number Generator on FPGA, IEEE Transactions on Instrumentation and Measurement 68 (1) (2019) 2018–2020.

[12] A. A. Rezk, A. H. Madian, A. G. Radwan, A. M. Soliman, Reconfigurable chaotic pseudo random number generator based on FPGA, AEUE - International Journal of Electronics and Communications 98 (1) (2019) 174–180.

[13] J. Cernak, Digital generators of chaos, Physics Letters A 214 (3-4) (1996) 151–160.

[14] S. Wang, W. Liu, H. Lu, J. Kuang, G. Hu, Periodicity of chaotic trajectories in realizations of finite computer pecisions and its implecation in chaos communications, International Journal of Modern Physics B 18 (19) (2008) 2617–2622.

[15] Y. Liu, H. Fan, E. Y. Xie, G. Cheng, C. Li, Deciphering an image cipher based on mixed transformed logistic maps, International Journal of Bifurcation and Chaos 25 (13) (2015) 1885–1896.

[16] D. Arroyo, G. Alverez, S. Li, C. Li, V. Fernandez, Cryptanalysis of a new chaotic cryptosystem based on ergodicity, International Journal of Modern Physics B 23 (05) (2009) 651–659.

[17] C. Li, D. Lin, J. Lu, Cryptanalyzing an image-scrambling encryption algorithm of pixel bits, IEEE Multimedia 24 (3) (2017) 64–71.

[18] Y. Zhang, D. Xiao, Cryptanalysis of s-box-only chaotic image ciphers against chosen plaintext attack, Nonlinear Dynamics 72 (4) (2013) 751–756.

[19] D. Arroyo, C. Li, S. Li, G. Alvarez, W. A. Halang, Cryptanalysis of an image encryption scheme based on a new total shuffling algorithm, Chaos, Solitons & Fractals 41 (5) (2009) 2613–2616.

[20] C. Li, K. T. Lo, Optimal quantitative cryptanalysis of permutation-only multimedia ciphers against plaintext attacks, Signal Processing 91 (4) (2011) 949–954.

[21] C. Li, S. Li, W. A. Halang, W. A. Halang, Cryptanalysis of an image encryption scheme based on a compound chaotic sequence, Image and Vision Computing 27 (8) (2009) 1035–1039.

[22] D. D. Wheeler, R. A. J. Matthews, Supercomputer investigations of a chaotic encryption algorithm, Cryptologia 15 (2) (1991) 140–152.

[23] G. Heidari-Bateni, C. D. Mcgillem, Chaotic direct-sequence spread-spectrum communication system, IEEE Transactions on Communications 42 (234) (1994) 1524–1527.

[24] Y. Zhou, Z. Hua, C. M. Pun, C. L. Chen, Cascade chaotic system with applications, IEEE Transactions on Cybernetics 45 (9) (2015) 2001–2012.

[25] K. W. Wong, S. H. Kwok, W. S. Law, A fast image encryption scheme based on chaotic standard map, Physics Letters A 372 (15) (2008) 2645–2652.

[26] X. Tong, Design of an image encryption scheme based on a multiple chaotic map, Communications in Nonlinear Science and Numerical Simulation 18 (7) (2013) 1725–1733.

[27] H. Hu, Y. Xu, Z. Zhu, A method of improving the properties of digital chaotic system, Chaos, Solitons & Fractals 38 (2) (2008) 439–446.

[28] L. Cao, Y. Luo, S. Qiu, J. Liu, A perturbation method to the tent map based on lyapunov exponent and its applicationa perturbation method to the tent map based on lyapunov exponent and its application, Chinese Physics B 24 (10) (2015) 78–85.

[29] S. Liu, J. Sun, Z. Xu, J. Liu, Digital chaotic sequence generator based on coupled chaotic systems, Chinese Physis B 18 (12) (2009) 5219–5227.

[30] L. Liu, S. Miao, A universal method for improving the dynamical degradation of a digital chaotic system, Physica Scripta 90 (8) (2015) 085205.

[31] X. Wang, L. Wang, A new perturbation method to the tent map and its application, Chinese Physis B 20 (5) (2011) 191–198.

[32] Z. Hua, Y. Zhou, Dynamic parameter-control chaotic system, IEEE Transactions on Cybernetics 46 (12) (2016) 3330–3341.

[33] Q. Wang, S. Yu, C. Li, J. Lü, X. Fang, C. Guyeux, J. M. Bahi, Theoretical design and fpga-based implementation of higher-dimensional digital chaotic systems, IEEE Transactions on Circuits & Systems I Regular Papers 63 (3) (2016) 401–412.

[34] K. Miyabayashi, O. Tonomura, M. Kano, S. Hasebe, Comparative study of state estimation of tubular microreactors using ukf and ekf, IFAC Proceedings Volumes 45 (15) (2012) 513–518.

[35] S. J. Julier, J. K. Uhlmann, Unscented filtering and nonlinear estimation, Proceedings of the IEEE 92 (3) (2004) 401–422.

[36] S. Sarkka, On unscented kalman filtering for state estimation of continuous-time nonlinear systems, IEEE Transactions on Automatic Control 52 (9) (2007) 1631–1641.

[37] L. Li, Q. Han, An UKF-based nonlinear system identification method using interpolation models and backward integration, Structural Control & Health Monitoring 25 (4) (2018) 1545–2263.

[38] Y. Liu, Y. Luo, S. Song, L. Cao, J. Liu, J. Harkin, Counteracting dynamical degradation of digital chaotic chebyshev map via perturbation, International Journal of Bifurcation and Chaos 27 (2017) 1–14.

[39] H. Hu, Y. Deng, L. Liu, Counteracting the dynamical degradation of digital chaos via hybrid control, Communications in Nonlinear Science and Numerical Simulation 19 (6) (2014) 1970–1984.

[40] Y. Deng, H. Hu, N. Xiong, W. Xiong, L. Liu, A general hybrid model for chaos robust synchronization and degradation reduction, Information Sciences 305 (2015) 146–164.

[41] L. Liu, J. Lin, S. Miao, B. Liu, A double perturbation method for reducing dynamical degradation of the digital baker map, International Journal of Bifurcation & Chaos 27 (7) (2017) 1750103.

[42] S. M. Pincus, Approximate entropy as a measure of system complexity, Proceedings of the National Academy of Science of the United States of America 88 (6) (1991) 2297–2301.

[43] A. Wolf, J. B. Swift, H. L. Swinney, J. A. Vastano, Determining Lyapunov exponents from a time series, Physica D Nonlinear Phenomena 16 (3) (1985) 285–317.

[44] M. T. Rosenstein, J. J. Collins, C. J. D. Luca, A practical method for calculating largest Lyapunov exponents from small data sets., Physica D-nonlinear Phenomena 65 (1-2) (1993) 117–134.

[45] J. P. Eckmann, S. O. Kamphorst, D. Ruelle, Recurrence plots of dynamical systems, Europhysics letters 4 (9) (1987) 973–977.

[46] A. L. Rukhin, statistical test suite for random and pseudorandom number generators for cryptographic applications, Applied Physics Letters 22 (7) (2010) 1645–179.

[47] P. L'Ecuyer, R. Simard, Testu01: A c library for empirical testing of random number generators, Acm Transactions on Mathematical Software 33 (4) (2007) 1–40.

[48] Y. Deng, H. Hu, W. Xiong, N. N. Xiong, L. Liu, Analysis and design of digital chaotic systems with desirable performance via feedback control, IEEE Transactions on Systems Man and Cybernetics Systems 45 (8) (2015) 1187–1200.

[49] X. Wang, Q. Xue, T. Lin, A novel true random number generator based on mouse movement and a one-dimensional chaotic map, Mathematical Problems in Engineering 2012 (2012) (2012) 95–100.

[50] H. Liu, X. Wang, Color image encryption based on one-time keys and robust chaotic maps, Computers and Mathematics with Applications 59 (10) (2010) 3320–3327.

[51] D. Lambić, Cryptanalyzing a novel pseudorandom number generator based on pseudorandomly enhanced logistic map, Nonlinear Dynamics 89 (1) (2017) 1–3.